Introdução à Criptografia e algoritmo RSA

Henrique Shodi Maeta

[1]Centro Universitário Senac, Santo Amaro

japa1996@hotmail.com

Abstract. *Transmit or receive confidential communication is not a recent necessity, and since antiquity it comes been developed new techniques of hidin and ciphering messages. Surrounded by many algorithms, we will deal with, in this article, in particular the RSA, that is one of the most secure and used cryptography algorithm nowadays.*

Resumo. *Transmitir ou receber comunicados sigilosos não é uma necessidade recente, e desde a atinguidade vêm sendo desenvolvidas novas técnicas de ocultação e cifragem de mensagens. Em meio à varios algoritmos trataremos neste artigo, em especial o RSA, que é um dos mais seguros e utilizados algoritmos de criptografia da atualidade.*

1. Introdução

Transmitir ou receber mensagens sigilosas não é uma necessidade recente, há relatos que na antiga Grécia eram utilizadas tábuas de madeiras, onde a mensagem era escrita, cobertas por cera, deste modo dificultaria o acesso e até mesmo a consciência de que a mensagem existia. Também, na Grécia antiga, dizem que um general raspava a cabeça de um escravo e alí gravava uma mensagem. Quando o cabelo do escravo estivesse escondendo a mensagem ele era levado para o destinatário, e, essa técnica recebeu o nome de esteganografia. Porém estas técnicas não eram muito eficientes, já que se o escravo fosse interceptado por outra pessoa ou fosse retirada a cera da tábua, não seria difícil achar estas mensagens.

Junto com a esteganografia uma outra técnica foi desenvolvida ao longo da história, tal técnica consistia em substituir cada letra da mensagem por uma outra letra, foi desenvolvida então, a cifra Atbash dos Hebreus por volta de 600 a.c., onde a primeira letra do alfabeto deveria ser substituída pela ultima, a segunda pela penultima e assim por diante (Figura 1 página 1).

ATBASH																									
CRIPTOGRAMA	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
SIGNIFICA	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figura 1. Exemplo Cifra de Atbash
[Sorian 2016]

Alguns anos depois Júlio César, líder militar e político romano, inventou a cifra de César, para se comunicar com seus generais de guerra, esta cifra consistia em deslocar o alfabeto uma determinada quantidade de vezes, e essa quantidade de vezes recebe o nome de chave, por exemplo, em uma mensagem encriptografada com a chave 1 na cifra de César a letra A será substituída pela B, a B pela C e assim por diante (Figura 2 página 2).

CIFRA DE CÉSAR																								
CRIPTOGRAMA	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
SIGNIFICA	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Figura 2. Exemplo de Cifra de César chave 3
[Sorian 2016]

Estas técnicas de criptografia se manteram por muito tempo até que Al-Kindi um matemático e filósofo árabe iniciou uma discução sobre técnicas de criptoanálise. Al-Kindi expecificou que, conhecendo a linguagem em que foi escrita a mensagem, para decifrá-la poderíamos utilizar o metodo de letras prováveis ou frequêntes (análise de frequência), por exemplo, um texto escrito em língua portuguesa a frequência na qual a letra A aparece é muito alta, então para decifrar o texto é necessário apenas verificar a constância em que as letras aparecem e assim descobrir a chave que foi utilizada para encriptografar e, consequêntemente, descobrir o texto original.

Por muitos anos foram sendo criadas novas maneiras de se encriptografar textos utilizando algoritmos de criptografia simétrica, onde uma mesma chave pode tanto criptografar quanto descriptografar uma mensagem (Figura 3 e Figura 4).

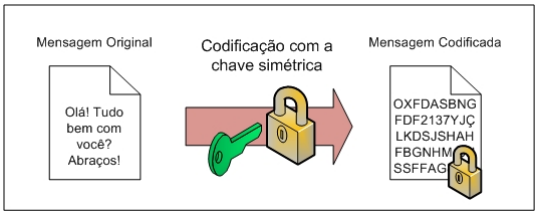

Figura 3. Chave simétrica usada para criptografar a mensagem
[Carvalho 2008]

Figura 4. Mesma chave usada, agora, para descriptografar a mensagem
[Carvalho 2008]

Um exemplo de criptografia simétrica é o algoritmo DES (Data Encryption Standard) com chave de 56 bits que foi criado pela IBM em 1977, porém em um desafio promovido pela internet e utilizando-se do método da tentativa e erro a segurança deste algoritmo foi quebrada. Porém este tipo de criptografia tinha um problema: Como combinar uma chave privada entre duas pessoas que querem se comunicar pela internet? A solução deste problema estava em um outro tipo de criptografia, a criptografia assimétrica que consiste em ter no mínimo duas chaves, uma para criptografar e outra para descriptografar (Figura 5 página 3 e Figura 6 página 3).

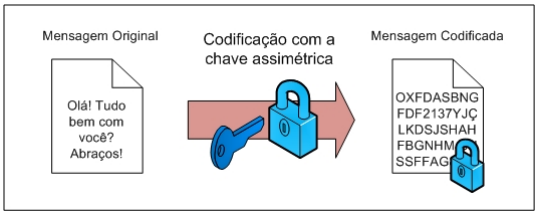

Figura 5. Chave azul para criptografar
[Carvalho 2008]

Figura 6. Chave amarela para descriptografar
[Carvalho 2008]

Então, problema de chaves no algoritmo simétrico foi resolvido, porém um algoritmo assimétrico é muito mais demorado, fazendo com que o desenvolvedor tenha que fazer uma escolha sábia, ponderando entre um algoritmo rápido porém não tão seguro, ou, um algoritmo lento, porém muito difícil de ser quebrado.

Um algoritmo de criptografia assimétrica que se destacou foi o RSA, que é muito utilizado em transações bancárias, e-commerce, e várias áreas na qual a segurança da informação é algo imprescindível, por conta da dificuldade de se obter a chave privada, mesmo sabendo como o algoritmo funciona.

2. Algoritmo RSA

Em 1978, três professores do Massachusetts Institute of Technology(MIT) publicaram um artigo entitulado ”A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”[Rivest et al. 1978] onde foi descrito um algoritmo para encriptografar e descriptografar uma mensagem utilizando números primos na ordem de, aproximadamente, 600 dígitos (como é recomendado, para que a segurança não falhe). Este algoritmo é muito seguro, pois é utilizado o produto de dois números primos, e a dificuldade de se fatorar este produto e obter os primos utilizados é uma tarefa tão ardua que para se descobrir os valores utilizados poderiam se levar anos, por conta de não possuirmos um algoritmo que nos faça este trabalho.

Para criptografar uma mensagem em RSA, devemos poder representar essa mensagem como um inteiro entre 0 e n - 1 são necessários dois números primos (p e q, que deverão ficar em segredo) o produto destes valores irá gerar a chave pública n então:

$$n = p * q$$

O próximo passo é calcular $\varphi(n) = (p-1) * (q-1)$ para podermos determinar a chave privada d que é determinada por:

$$\text{mdc}(d, \varphi) = 1$$

Ou seja, d e $\varphi(n)$ deverão ser primos entre si.

Sabendo d, o próximo passo é calcular a chave pública e que é dada por:

$$e * d \bmod \varphi(n) = 1$$

Tendo os valores de e, n e d, podemos então criptografar mensagens utilizando as chaves públicas da seguinte maneira:

$$M^e \bmod n = C$$

Onde M é a mensagem original, e C a mensagem cifrada. Para obtermos o texto original a partir do texto cifrado devemos utlizar:

$$C^d \bmod n = M$$

3. Conclusão

Desta forma podemos provar que o algoritmo RSA é muito seguro por conta da dificuldade de se obter os primos pela fatoração de seu produto e que tal dificuldade pode ser motivo para utilizar este algoritmo em aplicativos bancários, e-commerce, e-mails importantes entre outras muitas coisas, porém por trabalhar com números extensos a dificuldade de se computar estes dados aumenta de forma substancial, fazendo com que este algoritmo exija uma capacidade de processamento muito alta, pois caso contrário o processo pode se tornar muito demorado.

Referências

Al-Kadit, I. A. (1992). Origins of cryptology: the arab contributions. *Cryptologia*, 16(2):97–126.

Andrade, E. (2013). A história da criptografia. *Jornal PETNews*.

Carvalho, H. E. T. (2008). Pki - infra-estrutura de chaves públicas. `http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/hugo/Criptografia.html`. Accessed: 2016-04-26.

da Silveira, A. S. and Faleiros, A. C. (200?). Criptografia de chave pública - o papel da aritmética em precisão múltipla.

dos Santos, B. A. (200?). Criptografia rsa: Por quê esse método é tão seguro?

Oliveira, R. R. (2012). Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. *Segurança Digital*, 31:11–15.

Pisa, P. (2016). O que é criptografia? `http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html`. Acessed: 2016-04-26.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

Sorian, G. (2016). Criptogramas. `http://gravityfallsbrasil.blogspot.com.br/p/criptogramas.html`. Acessed: 2016-04-26.